UNITED STATES DISTRICT COURT FOR THE NOTHERN DISTRICT OF GEORGIA

Dallas Perkins, Jeffrey Pryor, Kenneth Yoeckel, and LaShawn Brown, and on behalf of themselves and all others similarly situated, Plaintiffs, v. Equifax Inc., Defendant.	Case No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Dallas Perkins, Jeffrey Pryor, Kenneth Yoeckel, and LaShawn Brown, ("Plaintiffs"), on behalf of themselves and all others similarly situated, file this Class Action Complaint ("Complaint") against Defendant Equifax Inc. ("Equifax" or "Defendant"), and respectfully allege the following:

NATURE OF THE ACTION

1. This class action seeks to redress Equifax's unlawful and negligent disclosure of millions of consumers' confidential personal identifying information ("PII"), including their names, birth dates, addresses, social security numbers, driver's license numbers, and credit card numbers in violation of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681 *et seq.*, Georgia data breach notification law, O.C.G.A. § 10-1-910 *et seq*, Georgia's Uniform Deceptive Trade Practices Act ("GUDTPA"), O.C.G.A. §§ 10-1-372, Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA"), FLA. STAT. § 501.204, Massachusetts' consumer protection law, MASS. GEN. LAWS 93A § 1 *et seq.*, New York's General Business Law § 349, and common law.

2. Defendant failed to fulfill its legal duty to protect consumers' PII which was stored in its systems. Equifax's willful, reckless, and negligent disregard for its obligations to

safeguard individuals' PII resulted in a massive data breach that occurred from mid-May through July of this year ("Data Breach" or "Breach").

3. Plaintiffs bring this action on behalf all persons who reside in the United States whose PII was compromised as a result of the Data Breach (the "Class" or "Class Members"), and, alternatively, on behalf of Florida, Georgia, Massachusetts, and New York residents whose PII was likewise compromised.

JURISDICTION AND VENUE

4. This Court has subject matter jurisdiction over Plaintiffs' claims pursuant to 28 U.S.C. § 1332(d) (CAFA) because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Equifax's citizenship, and (c) the matter in controversy exceeds $5 million, exclusive of interest and costs.

5. This Court has personal jurisdiction over Equifax because Equifax is a Georgia corporation and headquartered in Atlanta.

6. Venue is appropriate in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District.

PARTIES

7. Plaintiff Dallas Perkins is a resident of Cambridge, Massachusetts. After Mr. Perkins learned of the Data Breach, he immediately accessed Equifax's Breach website to check if his personal information was impacted by the Data Breach. Much to his dismay, according to Equifax's database, his personal information was compromised. After learning that his highly sensitive PII was exposed, Mr. Perkins purchased credit monitoring services from a third party to mitigate any injuries in connection with the Data Breach. Mr. Perkins intends to maintain credit monitoring services for the foreseeable future. While Mr. Perkins was aware that Equifax was

offering one complimentary year of TrustedID Premier to any U.S. persons interested in the service, in light of the fact that Equifax just jeopardized his and millions of other's highly sensitive information, Mr. Perkins did not trust that Equifax was sufficiently competent to protect his identity.

8. Plaintiff Jeffrey Pryor is a resident of Florida. After Mr. Pryor learned of the Data Breach, he immediately accessed Equifax's Breach website to check if his personal information was impacted by the Data Breach. Much to his dismay, according to Equifax's database, his personal information was compromised. After learning that his highly sensitive PII was exposed, Mr. Pryor intends to purchase credit monitoring services from a third party to mitigate any injuries in connection with the Data Breach. Mr. Pryor intends to maintain credit monitoring services for the foreseeable future. While Mr. Pryor was aware that Equifax was offering one complimentary year of TrustedID Premier to any U.S. persons interested in the service, in light of the fact that Equifax just jeopardized his and millions of other's highly sensitive information, Mr. Pryor did not trust that Equifax was sufficiently competent to protect his identity.

9. Plaintiff Kenneth Yoeckel is a resident of New York. After Mr. Yoeckel learned of the Data Breach, he immediately accessed Equifax's Breach website to check if his personal information was impacted by the Data Breach. Much to his dismay, according to Equifax's database, his personal information was compromised. After learning that his highly sensitive PII was exposed, Mr. Yoeckel purchased credit monitoring services from a third party to mitigate any injuries in connection with the Data Breach. Mr. Yoeckel intends to maintain credit monitoring services for the foreseeable future. While Mr. Yoeckel was aware that Equifax was offering one complimentary year of TrustedID Premier to any U.S. persons interested in the service, in light of the fact that Equifax just jeopardized his and millions of other's highly

sensitive information, Mr. Yoeckel did not trust that Equifax was sufficiently competent to protect his identity.

10. Plaintiff LaShawn Brown is a resident of Georgia. After Ms. Brown learned of the Data Breach, she immediately accessed Equifax's Breach website to check if her personal information was impacted by the Data Breach. Much to her dismay, according to Equifax's database, her personal information was compromised. While Ms. Brown was aware that Equifax was offering one complimentary year of TrustedID Premier to any U.S. persons interested in the service, in light of the fact that Equifax just jeopardized her and millions of other's highly sensitive information, Ms. Brown did not trust that Equifax was sufficiently competent to protect her identity.

11. Defendant Equifax, Inc. is incorporated under the laws of the State of Georgia, with its principal place of business in Atlanta, Georgia. Equifax operates through various subsidiaries, each of which acts as an agent of or in concert with Equifax.

FACTS

I. Equifax Data Breach

12. Equifax is one of three leading global consumer credit reporting agencies. Equifax provides a variety of informational services and resources for businesses, governments, and individuals. One segment of its services includes "consumer and commercial information services, such as credit information and credit scoring, credit modeling and portfolio analytics, locate, fraud detection and prevention, identity verification, and other consulting; mortgage loan origination information; financial marketing; and identity management services."[1]

[1] *Company Overview of Equifax Inc*, BLOOMBERG (Sept. 8, 2017), https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=175749.

13. As a credit reporting agency, in its regular course of business, Equifax collects and maintains a substantial amount of data on hundreds of millions of individuals.

14. Equifax provides products and services based on comprehensive databases of consumer and business information derived from a wide-range of sources including credit, financial assets, telecommunications and utility payments, employment, income, demographic, and marketing data.

15. According to its SEC filings, Equifax "rel[ies] extensively upon data from external sources to maintain our proprietary and non-proprietary databases, including data received from customers, strategic partners and various government and public record sources. This data includes the widespread and voluntary contribution of credit data from most lenders in the U.S and many other markets as well as the contribution of data under proprietary contractual agreements, such as employers' contribution of employment and income data to The Work Number, financial institutions' contribution of individual financial data to IXI, and telecommunications, cable and utility companies' contribution of payment and fraud data to the National Cable, Telecommunications and Utility Exchange."[2]

16. Consequently, the PII Equifax collects and maintains in the regular course of business, at the very least, includes information such as names, birth dates, addresses, phone numbers, driver's licenses, Social Security numbers, credit card accounts, loans, and lines of credit.

17. Equifax also offers "monitoring features for consumers who are concerned about identity theft and data breaches, including credit report monitoring from all three bureaus,

[2] Equifax, Inc., Annual Report (Form 10-K) (Feb. 22, 2017).

internet and bank account monitoring, lost wallet support, and the ability to lock and unlock the Equifax credit file."

18. Thus, PII and the security thereof are at the heart of Equifax's business.

19. Moreover, individuals and businesses who entrust Equifax with PII, which includes arguably *the most* sensitive PII available about any individual, do so with the understanding that Equifax will safeguard that information. That expectation is reinforced by Equifax's long-standing security guarantees to businesses, including financial institutions, who elect to use Equifax's services based on Equifax's promises to implement reasonable security measures to safeguard against theft and data breaches.

20. In a September 7, 2017 statement, Equifax revealed that data for approximately 143 million users was stolen from Defendant over a two and a half month period from mid-May to July 2017. [3]

21. The statement further revealed that Defendant initially discovered the Breach on July 29, 2017.[4]

22. According to the company, cybercriminals gained access to Equifax's databases by way of a vulnerability in its website.[5]

23. The Breach potentially compromised 143 million individuals' names, birth dates, addresses, social security numbers, and driver's license numbers, as well as roughly 209,000

---

[3] *See* Mohammed Hadi and Bryan Logan, *EQUIFAX: Hackers may have the personal details of 143 million US customers*, BUSINESS INSIDER (Feb. 7, 2017), http://www.businessinsider.com/equifax-hackers-may-have-accessed-personal-details-143-million-us-customers-2017-9.

[4] *See id.*

[5] *See id.*

U.S. consumers' credit card numbers and "certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers."[6]

24. At this time, it is unclear why it took approximately two and a half months for Equifax to discover the breach, or why it took the company nearly six weeks to inform victims of the Breach. Such a delay is damaging to the Breach's victims, in that they could have immediately acted in a manner to protect themselves and their PII from further harm.

II. Data Breaches Lead To Identity Theft

25. Data thieves intentionally hack into inadequately protected servers to steal PII with the primary incentive of weaponizing that private data to commit identity theft and financial fraud. Identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.

26. Given the scope of this Breach and the nature of the PII compromised, the ways in which criminals may unlawfully use the data is limitless, as is the timeframe for using the information for criminal endeavors.

27. Unfortunately for Plaintiffs and the Class, a person whose PII has been compromised may not fully experience the effects of the breach for years to come:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[7]

---

[6] *See id.*

[7] G.A.O., PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (June 2007), http://www.gao.gov/assets/270/262904.html.

28. The information implicated in the instant Breach is particularly susceptible to delay tactics in that an individual's name, address, driver's license, and Social Security number are not easily changed to mitigate risk over time. Accordingly, Plaintiffs and the Class Members will bear a heightened risk of identity theft or fraud for the unforeseeable future.

29. Identity theft occurs when an individuals' PII is used without his or her permission to commit fraud or other crimes.[8]

30. According to the Federal Trade Commission ("FTC"), "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[9]

31. As a direct and proximate result of Equifax's reckless and negligent actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, Plaintiffs and the Class are susceptible to identity theft.

32. The risks associated with identity theft are serious. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, banking or finance fraud, and government fraud. "While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information

---

[8] *See* FEDERAL TRADE COMMISSION: TAKING CHARGE: WHAT TO DO IF YOUR IDENTITY IS STOLEN (April 2013), https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

[9] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (March 2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

on their credit reports. In rare cases, they may even be arrested for crimes they did not commit."[10]

33. Having obtained the Plaintiffs' and Class Members' names, birth dates, addresses, driver's license numbers, and Social Security numbers, cybercriminals can use simply the data revealed or pair the data with other available information to commit a broad range of fraud in an victim's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money
- filing fraudulent tax returns;
- obtaining medical care and filing prescriptions;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

34. Beyond using the data exposed for nefarious purposes themselves, the cybercriminals who obtained Plaintiffs' and Class Members' PII may also exploit the data by selling it on the "black market" or "dark market" for years following a breach.

35. Indeed, there is a well-established international black market where hackers may quickly and efficiently sell -- in part or in whole -- precisely the type of PII stolen in the instant Data Breach.

[10] TRUE IDENTITY PROTECTION: IDENTITY THEFT OVERVIEW, http://www.idwatchdog.com/tikia//pdfs/Identity-Theft-Overview.pdf (visited Sept. 23, 2016).

36. Moreover, much like regular online marketplaces (such as eBay), many dark market websites (such as AlphaBay) include feedback systems for vendors, refund policies, and easily navigable search categories.[11]

37. The PII exposed in the Breach, which included, *inter alia*, names, birth dates, addresses, and Social Security numbers, qualifies as what hackers and black markets term as "fullz" records.[12] According to one 2015 estimate, the median price for someone's identity on the black market is approximately $21.35.[13] Fullz records are notably on the higher end of the pricing spectrum because they entail a "full set" of individuals' PII and the range of PII sold in the same markets also includes less glamorous information, such as basic credit card information.

38. Cybercriminals can further post stolen PII on the internet, thereby making such information publically available.

39. Moreover, individuals whose PII is subject to a reported security breach -- such as the Data Breach at issue here -- are approximately 9.5 times more likely than the general public to suffer identity fraud or identity theft.[14]

---

[11] Keith Collins, *Here's what your stolen identity goes for on the internet's black market*, QUARTZ, July 23, 2015, https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/.

[12] Brian Feldman, *So What Happens With All That Equifax Data?*, N.Y. MAGAZINE, Sept. 8, 2017, http://nymag.com/selectall/2017/09/so-what-happens-with-all-that-equifax-data.html.

[13] Keith Collins, *Here's what your stolen identity goes for on the internet's black market*, QUARTZ, July 23, 2015, https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/.

[14] See Javelin Strategy & Research, *Identity Fraud Industry Report: Social Media and Mobile Forming the New Fraud Frontier, available at* https://www.javelinstrategy.com/news/1314/92/1 (last visited Jun. 16, 2014).

III. Equifax Was Intimately Familiar With The Risks Of Cybersecurity Attacks

40. Equifax was well aware of the risk of cybersecurity attacks and data breaches.

41. Data security breaches -- and data security breach litigation -- dominated the headlines in 2015 and 2016 and continue to do so in 2017.[15]

42. Indeed, in May 2016, the chair of the U.S. Securities and Exchange Commission warned that cybersecurity is the biggest risk facing the financial system, and that corporate policies and procedures were not tailored to their particular risks.[16]

43. Perhaps the best example of a company's failure to tailor its policies and procedures to individualized risks is apparent here. Equifax, which knew how harmful a breach of its databases could be, failed to segregate sensitive data so that it was not all located in one place. As privacy and cybersecurity attorney Brenda Sharton explained, ""[h]ackers shouldn't be able to get 143 million people's information in one swoop."[17] Nevertheless, due to Equifax's failure to take reasonable precautions, they did.

44. Moreover, the vulnerabilities in Equifax's online software system Apache STRUTS and the resultant exploitations by hackers were widely recognized and reported for

---

[15] *See e.g.*, *Seagate Phish Exposes All Employee W-2*, KREBS ON SECURITY, March 6, 2016, https://krebsonsecurity.com/2016/03/seagate-phish-exposes-all-employee-w-2s/; Seth Fiegerman, *Yahoo Says 500 Million Accounts Stolen*, CNN TECH, Sept. 23, 2016, http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/.

[16] Lisa Lambert and Suzanne Barlyn, *SEC says cyber security biggest risk of financial system*, REUTERS, May 17, 2016, https://www.reuters.com/article/us-finance-summit-sec/sec-says-cyber-security-biggest-risk-to-financial-system-idUSKCN0Y82K4.

[17] Allison Grande, *Equifax's Massive Data Breach To Spur Uncharted Legal Woes*, LAW360, Sept. 8, 2017, http://www.law360.com/classaction/articles/962034.

months prior to the breach.[18] Equifax's failure to adequately remedy the flaws that it knew or should have known about its website containing highly sensitive PII was therefore negligent.

45. Equifax represented to the public that it understood the importance of protecting PII through robust security procedures. Equifax made representations regarding its ostensibly robust security practices in order to foster trust, and thus the provision of data necessary to provide its products and services, from individuals and businesses.

46. For instance, in its SEC filings, Equifax stated that it is "regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact."[19]

47. Equifax goes on to detail the risk posed by "security breaches" to its ability to provide its products and services, and recognizes that "[i]f data within our system is compromised by a breach, we may be subject to provisions of various state security breach laws[,]" as well as various federal and international laws.[20]

48. Equifax's negligence in safeguarding the PII with which it was entrusted is also exacerbated by the fact that the company's own website recognizes that "Data Breaches are on

[18] *See, e.g.*, Richard Chirgwin, *Apache Struts 2 bug bites Canada, Cisco, VMware and others*, The Register, March 14, 2017, https://www.theregister.co.uk/2017/03/14/canada_struts_2_outage/; Lucian Constantin, *Hackers exploit Apache Struts vulnerability to compromise corporate web servers*, PC WORLD, March 9, 2017, https://www.pcworld.com/article/3178660/security/hackers-exploit-apache-struts-vulnerability-to-compromise-corporate-web-servers.html.

[19] Equifax, Inc., Annual Report (Form 10-K) (Feb. 22, 2017).

[20] *Id.*

the rise," the importance of cyber security, and potential threats from hackers.[21]

49. Furthermore, this is not the first time the company has faced a data breach. Rather, Equifax has acknowledge or been implicated in previous data breaches, including smaller incidents in 2013 and 2015.[22]

IV. Plaintiffs and Class Members Suffered Damages As A Result Of The Data Breach

50. The Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiffs' and Class Members' PII against reasonably foreseeable threats to the security or integrity of such information.

51. Equifax failed to identify, implement, maintain, and monitor appropriate data security measures, polices, procedures, controls, protocols, and software and hardware systems to ensure the security of Plaintiffs' and Class Members' PII.

52. Additionally, Plaintiffs' and Class Members' PII was improperly handled, stored, segregated, and in some cases, either unencrypted or improperly partially encrypted, inadequately protected, readily able to be copied by data thieves, and not kept in accordance with basic security protocols.

53. Had Equifax taken appropriate security measures, the Data Breach would not have occurred.

---

[21] *See Data Breaches are on the rise. Be prepared.*, EQUIFAX, http://www.equifax.com/help/data-breach-solutions2/?HBX_PK=security_breach&HBX_OU=50 (last accessed Sept. 8, 2017); *Solutions: Equifax Breach Products*, EQUIFAX, http://www.equifax.com/business/equifax-breach-products/ (last accessed Sept. 8, 2017).

[22] Pierre Thomas, *Equifax Confirms Hackers Stole Financial Data, Launches Investigation*, ABC NEWS (Mar. 13, 2013), http://abcnews.go.com/Politics/equifax-confirms-hackers-stole-financial-data-launches-investigation/story?id=18715884; Letter from King & Spalding on behalf of Equifax to New Hampshire Attorney General Joseph Foster, regarding Data Incident Notification (Apr. 2, 2015), https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20150402.pdf.

54. Equifax's wrongful actions, inactions, and omissions directly and proximately caused the theft of Plaintiffs' and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harms for which they are entitled compensation, including, *inter alia*:

a. actual or attempted identity theft or fraud;

b. increased risk of harm, including actual identity theft and fraud;

c. the untimely and inadequate notification of the Data Breach;

d. improper disclosure of their PII;

e. diminution in the value of their PII;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of identity theft, identity fraud, and medical fraud;

h. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to mitigate or avert the increased risk of identity theft, identity fraud, and medical fraud;

55. To date, Equifax has not offered Plaintiffs and Class Members any compensation from the past, present, and future harm they may experience as a result of the Data Breach. Defendant has not offered any form of credit monitoring services besides, rather stunningly, a year of its own product, which Plaintiffs and Class Members may understandably distrust given the facts at issue in this litigation. To add insult to injury, after informing individuals that their most sensitive PII was revealed in the Breach, Equifax unconscionably requires that shocked, frightened, and vulnerable victims agree to an arbitration clause, which waives their rights to

bring or participate in a class action, class arbitration, or other representative action, or share in any class awards, in order to enroll in its credit monitoring service. Moreover, according to Equifax's monitoring service's Terms of Use, enrollments for Equifax's complementary service are subject to automatic renewal unless individuals proactively cancel their subscriptions.[23] Defendant has therefore not only failed to protect Plaintiffs and the Class Members against fraud and identity theft which may occur as a result of the Data Breach, but is instead using it to compel victims into forfeiting their rights and as an opportunity to profit by way of predatory practices.

CLASS ACTION ALLEGATIONS

56. Pursuant to FED. R. CIV. P. 23, Plaintiffs bring this action against Equifax as a class action on behalf of themselves and all members of the following nationwide class, or in the alternative, four state classes of similarly situated persons:

a. The Nationwide Class

All persons who reside in the United States whose PII was compromised as a result of the Data Breach.

b. The Georgia Class

All persons who reside in the State of Georgia whose PII was compromised as a result of the Data Breach.

c. The New York Class

All persons who reside in New York State whose PII was compromised as a result of the Data Breach.

d. The Florida Class

[23] *TrustedID Premier Terms of Use*, EQUIFAX, https://www.trustedid.com/premier/terms-of-use.php (last accessed Sept. 9, 2017).

All persons who ride in the State of Florida whose PII was compromised as a result of the Data Breach.

e. The Massachusetts Class

All persons who reside in the Commonwealth of Massachusetts whose PII was compromised as a result of the Data Breach.

57. All of the members of the classes and sub-classes are collectively referred to as the "Class" or "Class Members."

58. Plaintiffs reserve the right to modify or amend the Class definition before the court determines whether class certification is appropriate.

59. Excluded from the Class are: (i) Defendant and any entities in which Defendant has a controlling interest; (ii) any entities in which Defendant's officers, directors, or employees are employed and any of the legal representatives, heirs, successors, or assigns of Defendant; (iii) the Judge to whom this case is assigned and any member of the Judge's immediate family and any other judicial officer assigned to this case; and (iv) all governmental entities.

60. The members of the Class are so numerous that their joinder is impracticable. According to Equifax, there are 143 million of Class Members. Their identities, phone numbers, home addresses, and email addresses can be easily derived from Equifax's internal (and now external) records.

61. The rights of Plaintiffs and each Class Member were violated in precisely the same manner by Equifax's reckless and negligent actions, inaction, and omissions that caused the Data Breach and the unauthorized release and disclosure of their PII.

62. There are questions of law and fact common to the Class, as a whole. The common questions of law and fact predominate over any questions affecting only individual Members of the Class, and include, without limitation:

a. Whether Equifax had a duty to protect Plaintiffs' and the Class Members' PII;

b. Whether Equifax breached it duty to protect Plaintiffs' and the Class Members' PII;

c. Whether Equifax's breach of a legal duty caused its systems to be compromised, resulting in the loss and/or potential loss of over 143 million individuals' PII;

d. Whether Equifax properly designed, adopted, implemented, controlled, managed, and monitored data security processes, controls, policies, procedures and/or protocols to protect Plaintiffs' and the Class Members' PII in the Data Breach;

e. Whether Equifax failed to timely inform Plaintiffs and the Class Members of the Data Breach;

f. Whether Equifax's conduct was willful;

g. Whether Equifax's conduct was negligent; and

h. Whether Plaintiffs and Class Members are entitled to damages.

63. Plaintiffs' claims are typical of the claims of the Class Members because Plaintiffs, like all Class Members, is a victim of Equifax's wrongful actions, inaction, and omissions that caused the Data Breach, caused the unauthorized release and disclosure of their PII. Plaintiffs and their counsel will fairly and adequately represent the interests of the Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, other Class Members' interests. Plaintiffs' counsel is highly experienced in the prosecution of complex commercial litigation, consumer class actions, and data breach cases.

64. A class action provides a fair and efficient method, if not the only method, for adjudicating this controversy. The substantive claims of the representative Plaintiffs and the Class are nearly identical and will require evidentiary proof of the same kind and application of

the same law. There is no plain, speedy or adequate remedy other than by maintenance of this class action.

65. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because class members number in the thousands and individual joinder is impracticable. The expense and burden of individual litigation would make it impracticable or impossible for proposed class members to prosecute their claims individually. Trial of Plaintiffs' and the Class Members' claims is manageable. Unless the Class is certified, Defendant will remain free to continue to engage in the wrongful conduct alleged herein without consequence.

66. Certification of the Class, therefore, is appropriate under FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

67. Certification of the Class, also is appropriate under FED. R. CIV. P. 23(b)(2) because Equifax has acted, or refused to act, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or equitable relief with respect to the Class as a whole.

68. Certification of the Class, also is appropriate under FED. R. CIV. P. 23(b)(1) because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Equifax.

69. Equifax's wrongful actions, inaction, and omissions are generally applicable to the Class as a whole and, therefore, Plaintiffs also seeks equitable remedies for the Class.

70. Equifax's systemic policies and practices also make injunctive relief for the Class appropriate.

71. Absent a class action, Equifax will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury, and harm on Plaintiffs and Class Members.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Willful Violation of the Fair Credit Reporting Act

72. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

73. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

74. One of the fundamental purposes of FCRA is to protect consumers' privacy. 15 U.S.C. § 1681(a). Protecting consumers' privacy involves adopting reasonable procedures to keep sensitive information confidential. 15 U.S.C. § 1681(b).

75. FCRA defines a "consumer reporting agency" as:

> [A]ny person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

76. FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C. § 1681a(d)(1).

77. In the normal course of business and for monetary fees, Defendant assembles information about individuals, including, *inter alia*, names, birth dates, addresses, Social Security numbers, and driver's license numbers for the purpose of evaluating credit information or consumer reports for third parties.

78. Plaintiffs' and Class Members' PII constitute consumer reports under the FCRA because this information bears on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for: credit or insurance to be used primarily for personal, family, or household purposes; employment purposes; and any other authorized purposes.

79. FCRA requires the adoption of reasonable procedures with regard to, *inter alia*, the confidentiality and proper utilization of personal and insurance information. 15 U.S.C. § 1681(b). FCRA also requires that consumer reporting agencies "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e.

80. Defendant failed to adopt and maintain these and other reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b.

81. Defendant also failed to immediately notify Plaintiffs and Class Members about the Data Breach.

82. Equifax's failure to protect and safeguard Plaintiffs' and Class Members' PII resulted in the disclosure of such information to one or more third-parties in violation of FCRA because such disclosure was not necessary to carry out the purpose for which Equifax received

the information, nor was it permitted by statute, regulation, or order.

83. Defendant's violations of FCRA, as set forth above, were willful or, at the very least, reckless, constituting willfulness.

84. As a result of Defendant's willful or reckless failure to adopt and maintain reasonable procedures to limit the furnishing of Plaintiffs' and Class Members' PII to the purposes listed under 15 U.S.C. § 1681b, Plaintiffs' and the other Class Members' PII was disseminated to unauthorized third parties, compromised, and stolen. Plaintiffs suffered individual harm as a result of Defendant's willful or reckless violations of FCRA.

85. As a further direct or proximate result of Defendant's willful or reckless violations of FCRA, as described above, Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail above.

86. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages and statutory damages of not less than $100, and not more than $1,000, each, as well as attorneys' fees, punitive damages, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

SECOND CAUSE OF ACTION
Negligent Violation of the Fair Credit Reporting Act

87. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

88. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

89. Defendant negligently failed to adopt and maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes listed under 15 U.S.C. § 1681b.

90. Plaintiffs' and the other Class Members' PII was wrongfully disseminated to the public as a direct and foreseeable result of Defendant's failure to adopt and maintain such reasonable procedures.

91. Equifax's failure to protect and safeguard Plaintiffs' and Class Members' PII resulted in the disclosure of such information to one or more third-parties in violation of FCRA because such disclosure was not necessary to carry out the purpose for which Equifax received the information, nor was it permitted by statute, regulation, or order.

92. As a direct or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiffs' and Class Member's PII was made accessible to unauthorized third parties in the public domain, compromised, and stolen. Plaintiffs suffered individual harm as a result of Defendant's negligent violations of FCRA.

93. As a further direct or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail above.

94. Plaintiffs and the other Class Members, therefore, are entitled to compensation for their actual damages, as well as attorneys' fees, litigation expenses, and costs, pursuant to 15 U.S.C. § 1681o.

THIRD CAUSE OF ACTION
Negligence

95. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

96. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

97. Equifax had a duty to Plaintiffs and Class Members to safeguard and protect their PII.

98. Defendant assumed a duty of care commensurate with industry standards to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

99. Defendant had full knowledge about the sensitivity of Plaintiffs' and Class Members' PII, the PII's value to criminals, the increasing prevalence of data breaches, as well as the type of harm to could occur if such PII was wrongfully disclosed.

100. Defendant assumed a duty of care to use reasonable means to secure and safeguard this PII, to prevent its disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems.

101. Defendant also had a statutorily-imposed duty of care to protect the sensitive data with which it was entrusted by virtue of the FCRA. *See* O.C.G.A. § 51-1-6 ("When the law requires a person to perform an act for the benefit of another or to refrain from doing an act which may injure another . . . the injured party may recover for the breach of such legal duty if he suffers damage thereby.").

102. Defendant had a duty to use ordinary care in activities from which harm might be reasonably anticipated in connection with such highly sensitive PII data.

103. Defendant breached its duty of care by failing to secure and safeguard the PII of Plaintiffs and Class Members. Defendant negligently stored and/or maintained its systems.

104. Further, Defendant, by and through its above negligent actions and/or inaction, further breached its duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII within its possession, custody and control.

105. Plaintiffs and Class Members have suffered harm as a result of Defendant's negligence. These victims' loss of control over the compromised PII subjects each of them to a greatly enhanced risk of identity theft, fraud, and myriad other types of fraud and theft stemming from either use of the compromised information, or access to their user accounts.

106. It was reasonably foreseeable -- in that Defendant knew or should have known -- that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII would result in its release and disclosure to unauthorized third parties who, in turn wrongfully used such PII, or disseminated it to other fraudsters for their wrongful use and for no lawful purpose.

107. But for Defendant's negligent and wrongful breach of its responsibilities and duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

108. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiffs' and Class Members' PII, they have incurred (and will continue to incur) the above-referenced economic damages, and other actual injury and harm -- for which they are entitled to compensation. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

109. Plaintiffs and Class Members are entitled to injunctive relief as well as actual and punitive damages.

THIRD CAUSE OF ACTION
O.C.G.A. § 10-1-910 *et seq.*

110. Plaintiff Brown re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

111. Plaintiff Brown brings this claim on behalf of herself and the Georgia Class.

112. Section 10-1-912(a) of the Georgia Code provides, in pertinent part:

> Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay[.]

O.C.G.A. § 10-1-912(a).

113. The statute defines an "information broker" as any entity that, for monetary fees, "engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties[.]" O.C.G.A. § 10-1-911(3).

114. Moreover, in the event that more than 10,000 Georgia residents are impacted by the breach of security, the entity must also "notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis[.]" O.C.G.A. § 10-1-912(d).

115. The notification statute was established with the purpose of mitigating harms, as "[v]ictims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of unauthorized acquisition and possible misuse of a person's personal information is imperative." O.C.G.A. § 10-1-910(7).

116. Defendant qualifies as both an information broker, *i.e.*, an entity that collects personal information for the purpose of furnishing this information to third parties, that maintains computerized data, including individuals' PII, pursuant to the statute.

117. The Data Breach qualifies as a "breach of security of the system."

118. When Defendant learned of the Breach, Defendant knew that more than 10,000 Georgia residents' PII was implicated.

119. While Defendant discovered the Data Breach on July 29, 2017, it did not notify victims or other credit reporting agencies of the Breach until September 7, 2017 -- forty days later.

120. Defendant failed to notify Plaintiff, Class Members, and credit reporting agencies in the most expedient time possible and without unreasonable delay when it knew or reasonably believed that its databases were compromised.

121. Upon information and belief, no law enforcement agency instructed Defendant that notification to Plaintiff or Class Members would impede its investigation.

122. As the direct and proximate result of Equifax's unlawful delay in notification, Plaintiff and the Class Members sustained (and continue to sustain) injuries and damages as described above.

123. Accordingly, Plaintiff, on behalf of herself and the Class Members, respectfully request this Court award all relevant damages for Equifax's failure to timely notify Breach victims and credit reporting agencies of the Beach.

FOURTH CAUSE OF ACTION
Georgia's Uniform Deceptive Trade Practices Act

124. Plaintiff Brown re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

125. Plaintiff Brown brings this claim on behalf of herself and the Georgia Class.

126. Pursuant to Georgia's Uniform Trade Practices Act, O.C.G.A. § 10-1-372 of Georgia Code:

> (a) A person engages in a deceptive trade practice when, in the course of his business, vocation, or occupation, he: . . .
>
> (5) Represents that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have . . .
>
> (7) Represents that goods or services are of a particular standard, quality, or grade or that goods are of a particular style or model, if they are of another; . . .
>
> (9) Advertises goods or services with intent not to sell them as advertised; . . .
>
> (12) Engages in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.
>
> (b) In order to prevail in an action under this part, a complainant need not prove competition between the parties or actual confusion or misunderstanding.

O.C.G.A. § 10-1-372.

127. Defendant engaged in false and misleading representations to the public and to consumers (*i.e.*, individuals and entities seeking its services) concerning its data security in order to be entrusted with highly sensitive PII, which it received from a variety of sources including financial institutions, and in order to benefit financially.

128. In the course of Defendant's business, it willfully failed to disclose that its cybersecurity systems were inadequately protected and that its cybersecurity policies and procedures were inadequately implemented. In turn, Defendant willfully made affirmative representations that individuals' PII would be safe in its hands.

129. Furthermore, Defendant failed to timely disclose the Breach to Plaintiff and Class members; indeed, Equifax Has known for well over a month that the data was compromised.

130. Accordingly, Defendant made untrue, deceptive, and misleading representations of material facts and omitted and concealed material facts to the public, consumers, Plaintiff, and the Class.

131. In reality, Defendant failed to provide adequate protection for Plaintiff's and Class Members' PII, resulting in the Breach.

132. The security of Defendant's data systems was a material fact to Plaintiff and the Class. Had the public known of Defendant's misrepresentations and omissions as described herein, Defendant would not have been entrusted with the PII it has since compromised.

133. Plaintiff and the Class sustained (and continue to sustain) injuries and damages caused by Defendant's affirmative statements, as well as its failure to disclose material information, as described above.

134. Accordingly, Plaintiff, on behalf of herself and the Class Members, respectfully request this Court award equitable relief and attorneys' fees, as permitted by the statute. O.C.G.A. § 10-1-373.

FIFTH CAUSE OF ACTION
N.Y. GEN. BUS. LAW § 349

135. Plaintiff Yoeckel re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

136. Plaintiff brings this claim on behalf of himself and the New York Class.

137. New York General Business Law § 349 ("GBL 349") makes unlawful deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in this state.

138. Defendant engaged in false and misleading representations to the public and to consumers (*i.e.*, individuals and entities seeking its services) concerning its data security in order to be entrusted with highly sensitive PII, which it received from a variety of sources including financial institutions, and in order to benefit financially.

139. In the course of Defendant's business, trade, commerce or furnishing of any service, it willfully failed to disclose that its cybersecurity systems were inadequately protected and that its cybersecurity policies and procedures were inadequately implemented. In turn,

Defendant willfully made affirmative representations that individuals' PII would be safe in its hands.

140. Furthermore, Defendant failed to timely disclose the Breach to Plaintiff and Class members; indeed, Equifax Has known for well over a month that the data was compromised.

141. Accordingly, Defendant made untrue, deceptive, and misleading representations of material facts and omitted and concealed material facts to the public, consumers, Plaintiff, and the Class.

142. In reality, Defendant failed to provide adequate protection for Plaintiff's and Class Members' PII, resulting in the Breach.

143. The security of Defendant's data systems was a material fact to Plaintiff and the Class. Had the public known of Defendant's misrepresentations and omissions as described herein, Defendant would not have been entrusted with the PII it has since compromised.

144. Plaintiff and the Class sustained (and continue to sustain) injuries and damages caused by Defendant's affirmative statements, as well as its failure to disclose material information, as described above.

145. Pursuant to GBL 349, Plaintiff and the Class are entitled to recover the greater of actual damages or $50. Because Defendant acted willfully or knowingly as described herein, Plaintiff and the Class are entitled to recover three times their actual damages, up to $1,000.

SIXTH CAUSE OF ACTION
Florida Deceptive and Unfair Trade Practices Act

146. Plaintiff Pryor re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

147. Plaintiff Pryor brings this claim on behalf of himself and the Florida Class.

148. Section 501.204 of the Florida Statutes provides, in pertinent part:

> Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.

FLA. STAT. § 501.204.

149. Defendant engaged in false and misleading representations to the public and to consumers (*i.e.*, individuals and entities seeking its services) concerning its data security in order to be entrusted with highly sensitive PII, which it received from a variety of sources including financial institutions, and in order to benefit financially.

150. In the course of Defendant's trade or commerce, it willfully failed to disclose that its cybersecurity systems were inadequately protected and that its cybersecurity policies and procedures were inadequately implemented. In turn, Defendant willfully made affirmative representations that individuals' PII would be safe in its hands.

151. Furthermore, Defendant failed to timely disclose the Breach to Plaintiff and Class members; indeed, Equifax has known for well over a month that the data was compromised.

152. Accordingly, Defendant made untrue, deceptive, and misleading representations of material facts and omitted and concealed material facts to the public, consumers, Plaintiff, and the Class.

153. In reality, Defendant failed to provide adequate protection for Plaintiff's and Class Members' PII, resulting in the Breach.

154. The security of Defendant's data systems was a material fact to Plaintiff and the Class. Had the public known of Defendant's misrepresentations and omissions as described herein, Defendant would not have been entrusted with the PII it has since compromised.

155. Plaintiff and the Class sustained (and continue to sustain) injuries and damages caused by Defendant's unfair methods of competition, unconscionable acts and practices, and

unfair and deceptive acts and practices, including its affirmative statements, as well as its failure to disclose material information, as described above.

156. Accordingly, Plaintiff, on behalf of himself and the Class Members, respectfully request this Court award injunctive relief and all relevant damages.

SEVENTH CAUSE OF ACTION
MASS. GEN. LAWS 93A § 1 *et seq.*

157. Plaintiff Perkins re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

158. Plaintiff Perkins brings this claim on behalf of himself and the Massachusetts Class.

159. MASS. GEN. LAWS 93A § 2(a) declares unlawful "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."

160. Defendant engaged in false and misleading representations to the public and to consumers (*i.e.*, individuals and entities seeking its services) concerning its data security in order to be entrusted with highly sensitive PII, which it received from a variety of sources including financial institutions, and in order to benefit financially.

161. In the course of Defendant's trade or commerce, it willfully failed to disclose that its cybersecurity systems were inadequately protected and that its cybersecurity policies and procedures were inadequately implemented. In turn, Defendant willfully made affirmative representations that individuals' PII would be safe in its hands.

162. Furthermore, Defendant failed to timely disclose the Breach to Plaintiff and Class members; indeed, Equifax has known for well over a month that the data was compromised.

163. Accordingly, Defendant made untrue, deceptive, and misleading representations of material facts and omitted and concealed material facts to the public, consumers, Plaintiff, and

the Class.

164. In reality, Defendant failed to provide adequate protection for Plaintiff's and Class Members' PII, resulting in the Breach.

165. The security of Defendant's data systems was a material fact to Plaintiff and the Class. Had the public known of Defendant's misrepresentations and omissions as described herein, Defendant would not have been entrusted with the PII it has since compromised.

166. Plaintiff and the Class sustained (and continue to sustain) injuries and damages caused by Defendant's affirmative statements, as well as its failure to disclose material information, as described above.

167. Accordingly, Plaintiff, on behalf of himself and the Class Members, respectfully request this Court award all relevant damages for Equifax's unfair methods of competition, and unfair and deceptive practices.

EIGHTH CAUSE OF ACTION
Invasion of Privacy

168. Plaintiffs re-allege and incorporate by reference all preceding factual allegations as though fully set forth herein.

169. Plaintiffs bring this claim on behalf of themselves and the Class.

170. Plaintiffs' and Class Members' PII is private information.

171. Dissemination of Plaintiffs' and Class Members' PII would be offensive to a reasonable person.

172. The public has no legitimate interest in being apprised of Plaintiffs' and Class Member's PII.

173. Defendant's failure to safeguard and protect Plaintiffs' and Class Members' PII directly and proximately resulted in unreasonable publicity to the private lives of Plaintiffs' and

Class Members.

174. Plaintiffs' and Class Members' have a legal interest in the privacy of their PII.

175. Defendant's failure to safeguard and protect Plaintiffs' and Class Members' PII was a direct and proximate cause of the access to the PII and the obtaining of the PII as a matter of law.

176. Defendant's failure to safeguard and protect Plaintiffs' and Class Members' PII deprived Plaintiffs and Class Members of their legal interest in the privacy of that information, causing them damages.

177. As a result of Defendant's actions and inactions resulting in Plaintiffs' and Class Members' loss of privacy, Plaintiffs and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment as follows:

A. For an Order certifying the proposed Class pursuant to FED. R. CIV. P. 23(b)(1), (2) and/or (3); appointing Plaintiffs as Class Representatives for the nationwide Class and for each of their respective sub-classes; appointing Daniel DeWoskin of DEWOSKIN LAW FIRM, LLC, and Greg Blankinship and Jeremiah Frei-Pearson of FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP as Class Counsel;

B. For appropriate injunctive relief and declaratory relief, including an order requiring Defendant to immediately secure and fully encrypt all confidential information, to properly secure computers containing confidential information, to cease negligently storing, handling, and securing confidential information, and to provide identity theft monitoring for an additional five years;

C. Adjudging and decreeing that Defendant has engaged in the conduct alleged herein;

D. For compensatory and general damages according to proof on certain causes of action, as well as injunctive relief, and statutory, actual, and other applicable damages, including punitive damages;

E. For reimbursement, restitution and disgorgement on certain causes of action;

F. For both pre- and post-judgment interest at the maximum allowable rate on any amounts awarded;

G. For costs of the proceedings herein;

H. For an Order awarding Plaintiffs and the Class reasonable attorneys' fees and expenses for the costs of this suit; and

I. For any and all such other and further relief that this Court may deem just and proper, including but not limited to punitive or exemplary damages.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand trial by jury of all claims and causes of action in this lawsuit to which they is so entitled.

Dated: September 11, 2017 Respectfully submitted,

By: *s/ Daniel DeWoskin*
Daniel DeWoskin
Georgia Bar No. 220327
DEWOSKIN LAW FIRM, LLC
535 N. McDonough Street
Decatur, GA 30030
Telephone: (404) 987-0026
Fax: (404) 920-3341
dan@altantatrial.com

D. Greg Blankinship (*pro hac vice* forthcoming)
Jeremiah Frei-Pearson (*pro hac vice* forthcoming)
Chantal Khalil (*pro hac vice* forthcoming)
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP.
445 Hamilton Ave, Suite 605
White Plains, New York 10601
Telephone: (914) 298-3281
Fax: (914) 908-6709
gblankinship@fbfglaw.com
jfrei-pearson@fbfglaw.com
ckhalil@fbfglaw.com

Counsel for Plaintiffs and the Class